

Reply: [Full-Disclosure] Microsoft Windows Huge Text Processing Instability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/0722.html>

From: Kaveh Mofidi (*Admin_at_SecureTarget.Net*)

Date: 10/19/04

To: "'James Tucker'" <jftucker@gmail.com>

Date: Tue, 19 Oct 2004 09:27:43 +0330

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hi there,

There are no reason for answering your "obvious stupidities" when you are just in the middle of a nightmare!

Dear "James Tucker [jftucker@gmail.com]", I suggest to improve your imagination and just get out of your conventional thinking.

Before writing phrases like "how the * are you to exploit the system?" you should consider revising your mind on social communication and after that, you would probably be ready to exploit.

Have a nice dream,

Kaveh Mofidi

Head of Secure Target Network

<http://SECURETARGET.NET>

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.0.2

iQA/AwUBQXSszGO1siv41icpEQJAXACeObiJQQvf4lhiZESLbwqSXWbLvjAAAn3pb

iOZ1DYuoruY/+eK6qOZkv5V6

=EA+u

-----END PGP SIGNATURE-----

-----Original Message-----

From: James Tucker [mailto:jftucker@gmail.com]

Sent: Monday, October 18, 2004 2:28 PM

To: Kaveh Mofidi

Cc: ntbugtraq@listserv.ntbugtraq.com; full-disclosure@lists.netsys.com

Subject: Re: [Full-Disclosure] Microsoft Windows Huge Text Processing Instability

I am sorry, maybe I just don't get it, but the two forms you are talking about could not happen in the scenario described.

Besides this fact, user data space still has to be violated and this still requires either privileges (which means you have access anyway) or requires an exploit to elevate your privileges (again this makes the vector you describe pointless, it would only cause the ATTACKER issues).

There are some other VERY obvious stupidities here:

1. The system is described as "unstable" and "unresponsive" due to the load and virtual memory usage. Paging takes time and the system seems largely unresponsive whilst waiting for disk I/O. In this scenario, how the * are you to exploit the system? At the point of such high resource load that this becomes a problem the user will be unable to log out. Furthermore the attacker will be unable to log in / run programs unless they have taken control of the PC (not meaning personal computer, look up operating system principles (kernel design, in particular process and memory management) and assembler / machine coding if you dont know what it means).

2. This 'attack' is entirely dependant upon RAM volume. If the system in qu